PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-197293
(43)Date of publication of application : 16.08.1988

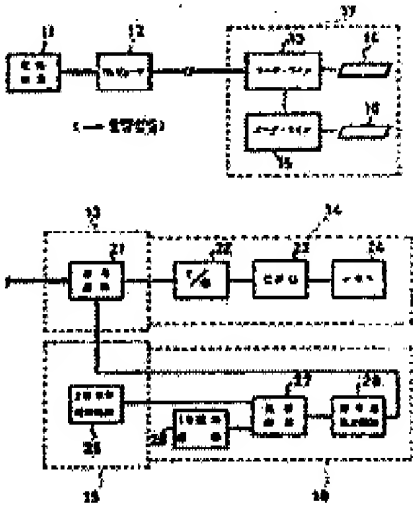
(51)Int.Cl. G06K 17/00
G07F 7/08

(21)Application number : 62-030400
(22)Date of filing : 12.02.1987

(71)Applicant : TOSHIBA CORP
(72)Inventor : KAMITAKE TAKASHI
ABE MASAHIRO
KAWAMURA SHINICHI

(54) IC CARD ISSUING SYSTEM

(57)Abstract:
PURPOSE: To form a publishing system for IC card with high security by ciphering the publishing information from a storing means through a transfer control means to an issuing information writing means.
CONSTITUTION: When an indication for starting the publishing operation is issued to a computer 12 by operating a first card reader/writer 13, the computer 12 reads the ciphered publishing information from a memory 11, and transferred to the first card reader/writer 13 through a communication circuit. When the operator inputs the ID number to a second card reader/writer 15, the ID number is collated by the ID number stored in a second IC card, and when both numbers coincide, a decoding key is outputted from a decoding key issuing circuit 28 and supplied to a decoder circuit 21. On the other hand, the decoder circuit 12 is inputted with a cipher-issuing information transmitted from the computer 12. Hence the decoder circuit 21 decodes the cipher issuing information by using the decoding key.



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－197293

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和63年(1988)8月16日
G 06 K 17/00		B－6711－5B	
		L－6711－5B	
G 07 F 7/08		M－6929－3E	審査請求　未請求　発明の数 1　（全5頁）

⑤4発明の名称　ＩＣカード発行システム

⑳特　願　昭62－30400
㉒出　願　昭62(1987)2月12日

⑦2発明者　神竹　孝至　神奈川県川崎市幸区小向東芝町1番地　株式会社東芝総合研究所内
⑦2発明者　阿部　雅宏　神奈川県川崎市幸区小向東芝町1番地　株式会社東芝総合研究所内
⑦2発明者　川村　信一　神奈川県川崎市幸区小向東芝町1番地　株式会社東芝総合研究所内
⑦1出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
⑦4代理人　弁理士　鈴江　武彦　外2名

明　細　書

1．発明の名称

ＩＣカード発行システム

2．特許請求の範囲

(1)　暗号化された発行情報を記憶する記憶手段と、この記憶手段に記憶された暗号化された発行情報の転送制御を行なう転送制御手段と、この転送制御手段の制御によって転送された前記暗号化された発行情報を復号鍵を用いて復号し、この復号化された発行情報を未発行ＩＣカードに書込む発行情報書込み手段と、この発行情報書込み手段に対してのみ前記復号鍵を与える復号鍵付与手段とを具備したこと特徴とするＩＣカード発行システム。

(2)　前記発行情報書込み手段は、発行用カードリーダ・ライタであることを特徴とする特許請求の範囲第1項記載のＩＣカード発行システム。

(3)　前記復号鍵付与手段は、鍵発生用カードリーダ・ライタと鍵発生用ＩＣカードとからなり、前記鍵発生用カードリーダ・ライタは、前記鍵発生用ＩＣカードを特定するＩＤ番号を出力し、前記鍵発生用ＩＣカードは、該ＩＣカードを特定するＩＤ番号を記憶するＩＤ記憶回路と、このＩＤ記憶回路に記憶されたＩＤ番号と前記鍵発生用カードリーダ・ライタから出力されるＩＤ番号とを比較する比較回路と、この比較回路での比較結果が一致したら前記復号鍵を送出する復号鍵送出回路とを具備したものであることを特徴とする特許請求の範囲第1項又は第2項記載のＩＣカード発行システム。

(4)　前記発行用カードリーダ・ライタと前記鍵発生用カードリーダ・ライタとは同一筐体に封止密閉されていることを特徴とする特許請求の範囲第3項記載のＩＣカード発行システム。

(5)　前記発行用カードリーダ・ライタと前記鍵発生用カードリーダ・ライタとを共用したことを特徴とする特許請求の範囲第3項記載のＩＣカード発行システム。

3．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

本発明は、カード発行時の安全性を高めたＩＣカード発行システムに関する。

（従来の技術）

ＩＣカードを発行するには、ＩＤ番号、サービス種目、カードの使用可能範囲等の発行情報を未発行のＩＣカードに対して書込む必要がある。この発行情報の中には、ＩＤ番号等の守秘を必要とする情報や改ざんされると不正使用されてしまう情報も含まれている。

これに対して、従来のＩＣカード発行システムは、例えば第５図にその概略を示すように、記憶装置１に記憶された発行情報をコンピュータ２の制御のもとでカードリーダ・ライタ３に転送し、このカードリーダ・ライタ３の図示しない挿入部に挿入された未発行のＩＣカード４に対して上記発行情報を書込むことが行われていた。

ところが、このようなシステムでは、不正なプログラムを与えることにより、記憶装置１から出力された生の発行情報をコンピュータ２で書き変える、或は生の発行情報をコピーして保存するといった操作をコンピュータ２に行なわせることができる。このため、発行情報を容易に盗んだり改ざんしたりすることが可能であった。

（発明が解決しようとする問題点）

このように、従来のＩＣカード発行システムでは、発行情報の転送制御を司る転送制御手段、例えばコンピュータのプログラムにより容易に発行情報を盗んだり改ざんできるという問題があった。

本発明は、このような問題点を解決すべくなされたもので、発行情報の転送制御を司る転送制御手段のプログラムをどのように組んでも発行情報が盗まれたり、改ざんされるおそれがないＩＣカード発行システムを提供することを目的とする。

［発明の構成］

（問題点を解決するための手段）

本発明は、記憶手段に生の発行情報を記憶させるのではなく、暗号化された発行情報を記憶させ、ＩＣカードに発行情報を書込む発行情報書込み手段は、転送制御手段の制御によって転送された前記暗号化された発行情報を復号鍵を用いて復号し、この復号化された発行情報を未発行ＩＣカードに書込むものとなっている。そして、本発明では、さらに前記発行情報書込み手段に対してのみ前記復号鍵を与える復号鍵付与手段が設けられている。

（作用）

本発明によれば、暗号化された発行情報を復号化するのに使用される復号鍵は、復号鍵付与手段から発行情報書込み手段にのみ与えられるので、復号化は発行情報書込み手段の内部でしか行なうことができない。したがって、もし転送制御装置が不正なプログラムで作動し、記憶手段から発行情報書込み手段に至る経路上で発行情報が盗まれても、これを復号化することができないので、生の発行情報を盗まれたり改ざんされたりすることがない。

（実施例）

以下、本発明の実施例について説明する。

第１図は本発明の一実施例に係るＩＣカード発行システムの構成を示すブロック図である。記憶装置１１は、予め図示しない暗号化回路により暗号化された発行情報（暗号発行情報）を記憶する。コンピュータ１２は転送制御手段となるものであり、記憶装置１１に記憶された暗号発行情報を、発行用の第１のカードリーダ・ライタ１３に転送する。第１のカードリーダ・ライタ１３は、受入れた暗号発行情報を後述する復号鍵を用いて復号化し、得られた生の発行情報を図示しない挿入部に受入れた未発行の第１のＩＣカード１４に書込む。

そして、このシステムには、上記発行用の第１のカードリーダ・ライタ１３及び第１のＩＣカード１４とは別個に復号鍵付与手段を構成する鍵発生用の第２のカードリーダ・ライタ１５と、第２のＩＣカード１６とが付加されている。

これら第１、第２のカードリーダ・ライタ１３，

１５及び第１、第２のＩＣカード１４，１６は、このシステムにおいてＩＣカードの発行端末１７として設けられており、コンピュータ１２には、このような発行端末１７が例えば通信回線を介して接続されることになる。なお、発行端末１７は、各々単一の第１、第２のカードリーダ・ライタ１３，１５からなるものに限定されるものではなく、複数の第１のカードリーダ・ライタ１３と単一の第２のカードリーダ・ライタ１５からなる場合、単一の第１のカードリーダ・ライタ１３と複数の第２のカードリーダ・ライタ１５とからなる場合、及び各々複数の第１、第２のカードリーダ・ライタ１３，１５からなる場合等、種々の構成をとることができる。

第２図は、上記発行端末１７の詳細ブロック図である。第１のカードリーダ・ライタ１３には、コンピュータ１２からの暗号発行情報を復号鍵を用いて復号する復号回路２１が設けられている。第１のＩＣカード１４には、上記復号回路２１で復号化された生の発行情報を入力するためのＩ／Ｏ回路２２と、このＩ／Ｏ回路２２を介して入力された発行情報の書込み制御を司るＣＰＵ２３と、このＣＰＵ２３の制御により生の発行情報を記憶するメモリ２４とが備えられている。また、第２のカードリーダ・ライタ１５には、カード発行のためにのみ使用される第２のＩＣカード１６を特定するＩＤ番号を、例えばオペレータの操作に基づいて送出するＩＤ番号送出回路２５が設けられている。そして、第２のＩＣカード１６には、そのＩＤカードを特定するＩＤ番号を記憶するＩＤ番号記憶回路２６と、このＩＤ番号記憶回路２６に記憶されたＩＤ番号と、前記ＩＤ番号送出回路２５から送出されるＩＤ番号とを比較し、一致したら一致信号を出力する比較回路２７と、この比較回路２７からの一致信号を入力して復号鍵を送出する復号鍵送出回路２８とを備えている。そして、復号鍵送出回路２８から出力される復号鍵は、第２のカードリーダ・ライタ１５を介して復号回路２１に直接与えられている。

以上のように構成された本実施例に係るＩＣカード発行システムにおいて、ＩＣカードの発行手続を行なうには、先ず、未発行状態の第１のＩＣカード１４を第１のカードリーダ・ライタ１３の図示しない挿入部へ、また鍵発生用の第２のＩＣカード１６を第２のカードリーダ・ライタ１５の図示しない挿入部へそれぞれ挿入する。

そして、第１のカードリーダ・ライタ１３の操作により、コンピュータ１２に対して発行作業開始の指示を与えると、コンピュータ１２は、記憶装置１１から当該ＩＣカード１４に関する暗号化された発行情報を読出し、これを通信回線を介して第１のカードリーダ・ライタ１３に転送する。

一方、オペレータが第２のカードリーダ・ライタ１５に対しＩＤ番号を入力すると、第２のＩＣカード１６の内部でこの入力されたＩＤ番号と内部に記憶されたＩＤ番号との照合を行ない、両者が一致していれば復号鍵送出回路２８から復号鍵が出力される。この復号鍵は、復号回路２１に与えられる。

一方、復号回路２１には、コンピュータ１２により転送された暗号発行情報が与えられている。したがって、復号回路２１は、この暗号発行情報を上記復号鍵を用いて復号化する。このようにして復号化された生の発行情報は、Ｉ／Ｏ回路２２、ＣＰＵ２３を介してＩＣカード１４の内部のメモリ２４に格納される。

以上の手順により生の発行情報がＩＣカード１４の内部に格納されることになる。そして、一度メモリ２４に格納された発行情報については、読出すことも書き変えることもできない。

本実施例に係るシステムによれば、記憶装置１１～コンピュータ１２～第１のカードリーダ・ライタ１３の各経路上の発行情報が暗号化されているので、たとえコンピュータ１２に不正なプログラムを与えて発行情報を盗んでも、これを復号化することができない。このため、生の発行情報をが知られることはない。また、暗号化された発行情報を改ざんしようとしても、復号鍵が知られない限り、改ざんされた内容に、特定の意味を持たせることができないので、そのような改ざんに

よってＩＣカード１４を不正に使用するという企ては成功しない。したがって、このシステムによれば、カード発行時の安全性を高めることができる。特に、このシステムでは、復号鍵付与手段として第２のＩＣカード１６を設け、復号鍵をこのＩＣカード１６の内部から発生させるようにしているので、第２のカードリーダ・ライタ１５内に直接復号鍵を入力することによる危険を回避できる。しかも、このシステムでは復号鍵発生のために、ＩＣカード１６とＩＤ番号の入力とを必要としているので、２重の安全性が図れるなどの効果を奏する。

なお、上記実施例では、発行端末を構成する第１、第２のカードリーダ・ライタ１３，１５を別々に設けたが、第２のカードリーダ・ライタ１５から第１のカードリーダ・ライタ１３に与えられる復号鍵が万一盗まれる危険性を考慮した場合には、例えば第３図に示すように、上記２つのカードリーダ・ライタ１３，１５を１つのカードリーダライタ３１にまとめることが望ましい。この場合には、例えば２つのカードリーダ・ライタを１つの筐体で封止密閉しておくことが好ましい。

また、発行用カードリーダ・ライタと鍵発生用カードリーダ・ライタとを１つのカードリーダ・ライタ３２として完全に共用する場合には、第４図に示すように、まず第２のＩＣカード１６をカードリーダ・ライタ３２に挿入して復号鍵を読出し、続いて第１のＩＣカード１３を挿入して発行操作を行なうようにすれば良い。

さらに、以上の各実施例では、復号鍵付与手段として鍵発生用のカードリーダ・ライタと鍵発生用のＩＣカードとを用いたが、このような手段を用いなくても、例えば復号鍵をオペレータ操作で直接入力しても良い。このような構成によっても従来のシステムに比較した安全性向上は十分に見込まれる。

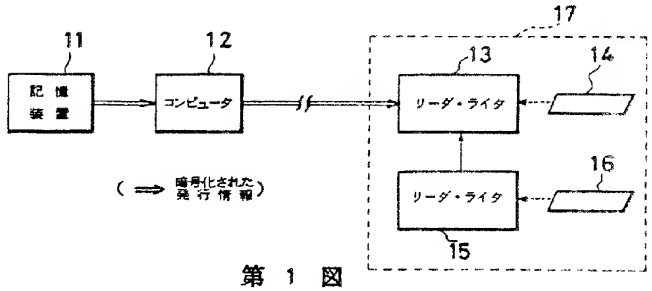
［発明の効果］

以上述べたように、本発明によれば、記憶手段から転送制御手段を介して発行情報書込み手段に至る発行情報が暗号化されているので、生の発行情報が盗まれたり改ざんされるおそれがない。このため、安全性の高いＩＣカード発行システムを提供することができる。

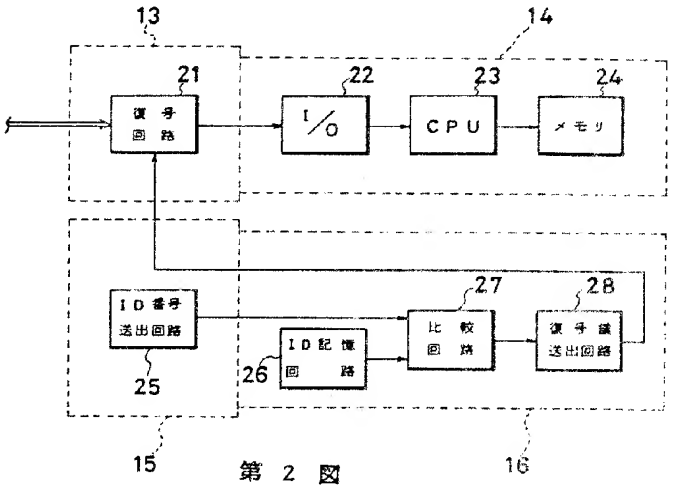
４．図面の簡単な説明

第１図は本発明の一実施例に係るＩＣカード発行システムの構成を示すブロック図、第２図は同システムにおける発行端末のさらに詳細なブロック図、第３図及び第４図は本発明のそれぞれ他の実施例に係るＩＣカード発行システムの構成を示すブロック図、第５図は従来のＩＣカード発行システムの構成を示すブロック図である。

１，１１…記憶装置、２，１２…コンピュータ、３，３１，３２…カードリーダ・ライタ、１３…第１のカードリーダ・ライタ、１４…第１のＩＣカード、１５…第２のカードリーダ・ライタ、１６…第２のＩＣカード。

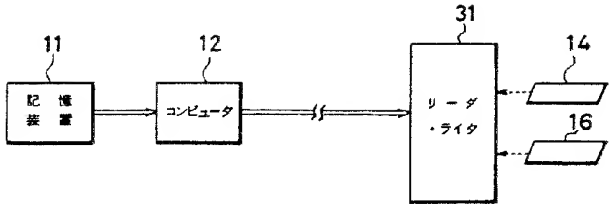


第１図

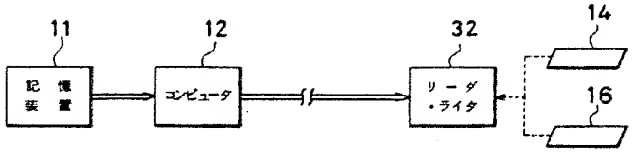


第２図

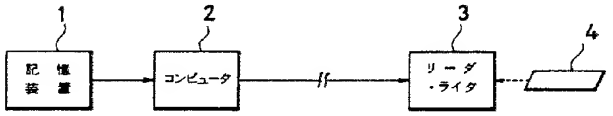
出願人代理人　弁理士　鈴江武彦


11
12
31
14
16
記憶装置
コンピュータ
リーダ・ライタ

第 3 図


11
12
32
14
16
記憶装置
コンピュータ
リーダ・ライタ

第 4 図


1
2
3
4
記憶装置
コンピュータ
リーダ・ライタ

第 5 図